



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/672,184	09/25/2003	Eduard K. de Jong	SUN-040027	9837
24209	7590	02/08/2008	EXAMINER	
GUNNISON MCKAY & HODGSON, LLP			PICH, PONNOREAY	
1900 GARDEN ROAD			ART UNIT	PAPER NUMBER
SUITE 220			2135	
MONTEREY, CA 93940			MAIL DATE	DELIVERY MODE
			02/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

**Advisory Action
Before the Filing of an Appeal Brief**

Application No.

10/672,184

Applicant(s)

DE JONG, EDUARD K.

Examiner

Ponnoreay Pich

Art Unit

2135

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 24 January 2008 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) The period for reply expires _____ months from the mailing date of the final rejection.
- b) The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because

- (a) They raise new issues that would require further consideration and/or search (see NOTE below);
- (b) They raise the issue of new matter (see NOTE below);
- (c) They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
- (d) They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. Applicant's reply has overcome the following rejection(s): _____.

6. Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. For purposes of appeal, the proposed amendment(s): ~~a) will not be entered, or b) will be entered and an explanation of~~ how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: _____.

Claim(s) objected to: _____.

Claim(s) rejected: 1-4, 6-9, 11-14 and 16-19.

Claim(s) withdrawn from consideration: 5, 10, 15 and 20.

AFFIDAVIT OR OTHER EVIDENCE

8. The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. The request for reconsideration has been considered but does NOT place the application in condition for allowance because: see attached.

12. Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____.

13. Other: _____.

Response to Arguments

Applicant's arguments submitted on 1/24/08 were fully considered, but were not persuasive.

Applicant once again argues that the restriction of the claims should be withdrawn. Applicant states the groups having different limitations are insufficient to show two way distinctness. The examiner respectfully submits that not only do groups I and II have distinct limitations, but they also have separate utilities as explained when the restriction requirement was made. Group I (claims 1-4, 6-9, 11-14, and 16-19) have utility for program obfuscation while group II (claims 5, 10, 15, and 20) have separate utility such as program decryption. Since each group of inventions have distinct limitations not found in the other subcombination, the subcombinations (group I and group II) do not overlap in scope and are not obvious variants. Each subcombinations have also been shown to be separately usable as evidenced by their separate utilities. As such, each subcombinations have been shown to be two way distinct (see MPEP 806.05(d)), thus restrictable.

Applicant argues that the 103 rejection of claims 1, 6, 11, and 16 confuses two parts of Kessler and arbitrarily extract teachings from different parts and then recombine them. Applicant states that the rejection relies upon the proprietary client software and teachings about how a TK is processed to support file transfer in a peer to peer network, which applicant argues are two different and distinct things as taught by Kessler. The examiner respectfully disagrees. Kessler taught that the proprietary client software is used to facilitate file sharing (col 4, lines 44-46). Kessler then proceeded to

discuss various ways the proprietary client software could be used to share files using different keys, one of which is key TK (col 9, lines 26-52). TK is used with the proprietary client software for file transfer along with the public/secret key pair of the client, thus applicant's argument that the teaching of TK and the proprietary client software are unrelated is incorrect.

On page 5 of the remarks submitted, applicant recognizes that Kessler teaches that the obfuscation algorithm, de-obfuscation algorithm, the secret key, and the public key are themselves obfuscated and/or encrypted within the proprietary client software, however, applicant argues that Kessler fails to teach how the various elements of Kessler are obfuscated and/or encrypted within the proprietary client software before that software is transferred to a client. It is unclear what point applicant is trying to make with this argument. If applicant is trying to state that applicant is claiming a specific type of obfuscation method while Kessler does not get into the specifics of how his invention obfuscates, then it should be recognized that applicant cannot overcome an obviousness rejection that is based on more than one references by attacking a single reference by itself. Kessler teaches that various algorithms and keys are obfuscated and/or encrypted into the proprietary client software. The additional teachings of Okada, Shen Orr and LeVine were relied upon to cover the more specific details of how such obfuscation and/or encryption may be accomplished.

Applicant argues that Kessler describes that the key TK is not included in the proprietary client software, thus the combination of the proprietary client software and the key TK changes the principles of operation of Kessler because there is no citation of

an encrypted key TK being scrambled with the proprietary client software. The examiner respectfully submits that the principle operation of Kessler's invention is directed towards the encryption and transferring of files (see abstract). It is unclear how including TK with the proprietary client software (as per Shen Orr's additional teachings) would prevent this since both the sender and receiver need TK in order to accomplish the sending and receiving of files and the encryption and decryption of those files. Based on applicant's argument, the principle operation of an invention is always changed if the reference does not teach every limitation being claimed. Applicant's argument essentially removes 35 USC 103 from consideration in determining patentability of a claim since applicant is essentially arguing that if the reference doesn't explicitly teach something, it is not obvious and any attempt to modify the teachings of the reference according to the teachings of another reference changes the principle operation of the invention, therefore shouldn't be done.

Applicant argues that the plain meaning of "scrambling...said encrypted second cryptographic key into said instruction stream using a code obfuscation method indicated by an obfuscation descriptor" was not considered by the examiner. The examiner respectfully disagrees. Shen Orr's additional teaching was relied upon to disclose creating an obfuscated key description program (p16, line 31-p17, line 3; p21, lines 1-2; and p24, lines 17-19) via use of an code obfuscation method and an obfuscation descriptor (p9, lines 19-24 and p9, line 33-p10, line 2). LeVine's additional teachings were relied upon to make obvious that the code obfuscation method used involves scrambling an encrypted key into the instruction stream of a program

(paragraphs 12, 21, 23, 26, and 78). It was noted in the last office action that based on these teachings by Shen Orr and LeVine, the limitation of "scrambling ... said encrypted second cryptographic key into said instruction stream using a code obfuscation method indicated by an obfuscated descriptor" was considered obvious. The rationales for why it would have been obvious to combine these teachings were also discussed in the last office action. As such, the plain meaning of the limitation was considered.

Applicant argues that the rejection does not identify an instruction stream that is a key decryption program configured to perform said decryption algorithm for said cryptographic key and that has an encrypted key scrambled into the instruction stream to obtain an obfuscated instruction stream. The examiner respectfully submits that it appears that applicant has only considered each individual references used in the rejection by themselves rather than what the references as a whole would make obvious. One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Kessler discloses that the proprietary client software has embedded decryption algorithms (col 8, lines 51-53). The embedded decryption algorithms were explained in the rejection (see page 7) as being considered the instruction stream that has a key decryption program configured to perform said decryption algorithm for said first cryptographic (col 8, lines 50-67 and col 10, lines 58-67). Further as explained above, the teachings of Shen Orr and LeVine were relied upon to establish that it would have been obvious to modify the embedded decryption algorithms of Kessler such that

it has an encrypted key scrambled into its instruction stream thereby obtaining an obfuscated instruction stream.

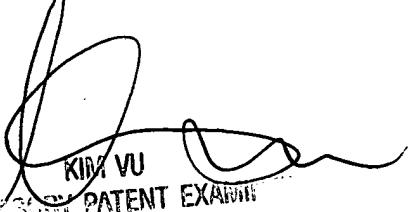
Applicant states that Kessler taught that the obfuscation of encrypted TK was unnecessary. The examiner respectfully submits that there does not appear to be any disclosure by Kessler where he states that.

Applicant argues that the public key PK and secret key SK was needed to make file transfer work, thus use of other key combination (i.e. TK) would break Kessler because the public key PK and secret key SK combination is gone. The examiner respectfully disagrees. Kessler's invention actually requires use of other keys, i.e. TK, for file transfer. Figure 2 shows that each client contains a respective public and secret key pair (i.e. PK1, SK1, PK2, and SK2). One skilled should understand that in public key cryptography, a file that has been encrypted using a public key can only be decrypted using the corresponding secret/private key. In other words PK and SK referred to by Kessler are public/private key pairs. The clients, having these keys, are disclosed by Kessler as also using TK for file transfer (Fig 3; col 5, lines 29-42; and col 6, lines 52-65). Since use of TK is required to make Kessler's invention work, it's use would not remove PK and SK from his invention and break the invention. In Kessler's invention, the public/private key pair is used to transfer TK from one client to the other while TK itself is used to encrypt/decrypt the file being transferred, i.e. musicfile.mp3.

Applicant argues that the rejection confuses the proprietary client software with the process for transferring files between clients as taught by Kessler. The examiner respectfully disagrees. The public key PK and secret key SK are used to transfer TK

from one client to the other while TK itself is used to encrypt the data file being transferred (col 5, lines 43-47 and Fig 3). The proprietary software contains the public and secret keys (col 8, lines 50-53) used to enable secure transfer of TK from one client to the other, thus it is impossible to consider file transfer as taught by Kessler without considering the proprietary client software which contains the keys needed for the transfer process.

Applicant's remaining arguments are directed towards dependency. However, because the arguments for the independent claims are traversed, the dependent claims are also not allowable.



KIM VU
USPTO PATENT EXAMINER
TECHNOLOGY CENTER 2100